

REMARKS/ARGUMENTS

The present application discloses a document repository system in which the originator of the document is able to ensure the integrity and security of its document filed with a third party repository without having to trust the administrator of that repository. In this repository system, the document originator and the repository administrator have vault environments which are secure extensions of their respective work spaces. The vault of the document originator encrypts a document that it receives from the originator, prior to forwarding it on to the vault of the repository to maintain the document secure from the repository administrator. When a request is made to view the document, it is made from the vault which is a secure extension of the requesting party's work space to the repository's vault. The repository's vault retrieves a copy of the encrypted document which is forwards, along with the requester's identity, to the originator's vault. The originator's vault verifies that the requester is authorized to view the document from the access control list using an access control list identifying access ownership privileges for the document stored in the vault itself. The originator's vault decrypts the document and forwards the decrypted document directly to the requester's vault. Therefore the repository administrator never handles the decrypted documents or the encrypting and decrypting of the documents.

The repository system also maintains the information on authorized user access secure from any actions of the third party administrator of the repository. To this end, the system includes a communications environment that houses a first agent program in the data repository system which is a secure extension of the work space of the depositor's computer and a second agent program which is a secure

extension of the work space of a first user computer with access privileges to the electronic data file. The first user computer has a record of its access privileges to the electronic data file which is accessible to and maintained by the second agent program. When changes are made to the manifest affecting the first user computer's access privileges to the electronic data file, these changes are communicated from the first agent program to the second agent program so that the first user computer's record of its access privileges can be updated. The first agent program is also able to verify the first user computer's access privileges to the electronic data file before the electronic data file is released to the second agent program.

Claim Rejections Under 35 USC 103

Claims 1, 3-4, and 6-15 in the application were all rejected under 35 USC 103(a) as being unpatentable over the Frisch reference entitled "Essential system Administration" 2nd Edition in view of Garfinkel Practical UNIX Security, both references being published by O'Reilly & Associates, Inc.

Neither the Frisch or Garfinkel references teach excluding access to system administrators from vaults of originators and users in the manner described above. As pointed out previously, page 226 of the Frisch reference discusses the system administrators ability in NFS to grant "ROOT" access to an account. Therefore, the administrator could grant him/herself such access. Further, material beginning on page 246 of the Frisch reference makes it clear that a repository administrator in NFS has access to a directory when running a program called "CRACK". Therefore the repository administrator in a third party repository would have access to the user's directory with CRACK. Even the Examiner has pointed out that the

Frisch reference does not “disclose means of establishing a secure extension of each computer of a plurality of computers”.

The Examiner relies on the Garfinkel reference to make up for the Frisch reference failures. The Examiner still argues that NFS affords a secure extension for NFS mounted file systems, pointing to pages 264 to 266 of the Garfinkel article. However, after these pages on page 272, Garfinkel recommends that if concerns about security are paramount perhaps the user should not use NFS. Further, nothing is said in these pages about negating the administrators ability in NFS to obtain access to a user’s account by granting itself ROOT access. Therefore, pages 264 to 266 do not change the fact that the Frisch and Garfinkel articles make it abundantly clear that materials resident in an NFS system are not too secure.

The applicant’s attorney found nothing on page 64 of the the Garfinkel article about restricting the access of a repository administrator to a directory of authorized users for data stored in the repository. While page 64 talks about changing users privileges to a file, there is no mention of a repository administrator’s ability to gain access to a user’s directory by running the CRACK program mentioned in Frisch. Therefore there is nothing in the Frisch and Garfinkel articles teaching restricting an administrator’s access by having user’s directories and software for maintenance and updating of access privileges held in vaults that are secure extensions of the depositor’s and user’s computers which are free from access by the repository manager. For those reasons the combination of the Frisch and Garfinkel articles does not teach the above described manner of restricting of the administrators ability to enter the user’s account and get access to its directory

since Garfinkel does not suggest, to those skilled in the art, modification of the Frisch reference as proposed by the Examiner.

Because the article does not teach the described manner of restricting the ability of the administrator to enter the depositor's and user's accounts, it is unlikely that those skilled in the art would combine the Frisch and Garfinkel references for that purpose. Additionally, those skilled in the art would be unlikely to combine the teachings of Frisch and Garfinkel because the Garfinkel article makes it clear that materials resident in an NFS system are not secure and directs people concerned about security not to use NFS.

All claims in the application are allowable over the Frisch and Garfinkel references for the reasons discussed above. For instance, claim 1 calls for a system restricting access by the repository system administrator to lists of access privileges to electronic data files of a document depositor by having a program relating to maintaining and updating a manifest of access privileges in a secure extension of the depositor computer and a second agent program maintaining a record of a first user's access privileges in a secure extension of the first user computer. As pointed out above, the repository administrator in the Frisch and Garfinkel combination has access to such lists when running the CRACK and/or ROOT program.

Independent claims 10 and 14 both call for a data repository having the originator's of the electronic data files, user's electronic data files, and the administrators of the electronic files provided with vaults which are secure extensions of their respective work spaces so that data and directories for that data are secure from the repository administrator. (Changes in claims 10 and 14 do not

constitute new issues since they reflect the language contained in now cancelled dependent claims 18 and 20, respectively.)

Independent claims 11 and 12 both call for maintaining records relating to document access that are secure to the document originator and secure from the repository administrator.

Dependent claims further distinguish from the prior art. For instance, claim 4 adds a third agent program which is a secure extension of a second user computer containing a record of the second user's computer access privileges.

Claim Objections

Claims 1 and 3 have been amended in light of the Examiner's remarks while the language in new claims 22 and 23 take in account those remarks.

Claim Rejections under 35 USC 112

Claim 17 has been amended to eliminate any indefiniteness including changing "the vault" to "a vault" in the occurrences mentioned by the Examiner.

Allowable Subject Matter

The Examiner has stated that claim 17 would be allowable if corrected to overcome the rejection under 35 USC 112. As pointed out above, claim 17 has been amended for that purpose. The Examiner has indicated that the subject matter

of claims 19 and 21 would be allowable in independent form. Therefore new claim 22 should be allowable since it incorporates the subject matter contained in claim 19 in independent form and claim 23 should be allowable since it contains the subject matter of claim 21 in independent claim form.

For the above reasons, it is respectfully submitted that the claims are allowable over the prior art and the application is in condition for allowance. Therefore, it is requested that the application be reconsidered, allowed and passed to issue.

Respectfully submitted,



James E. Murray - Attorney
Reg. No.: 20,915
Telephone No.: (845) 462-4763